REMARKS

Reconsideration of this application, as amended, is earnestly requested.

Claims 1, 5, 10, and 22 are amended in this paper as shown above. Claim 4 is cancelled without prejudice, and claims 25-27 are added

Claims 1, 2, 4-11, and 14-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Wasilewski (US 5,420,866) in view of Daemen ("AES Proposal: Rijndael," March 1999), and claims 3 and 12-13 as being unpatentable over Wasilewski in view of Daemen and further in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000). These rejections are respectfully traversed.

Independent claims 1, 10, and 22 have been amended to recite the limitation "wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit." This limitation adds no new matter and finds support in the specification in at least paragraphs 0047 and 0061. Independent claim 1, as amended, now recites:

> An apparatus for encrypting/decrypting a real-time input stream, comprising:
>
> a control unit receiving a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream into data blocks, providing the data blocks for encryption or decryption, receiving encrypted or decrypted data blocks, converting the received encrypted or decrypted data blocks into bytes, and outputting the bytes;
>
> a key schedule unit carrying out a key schedule for every round in accordance with a variable key size so as to output a key for the encryption or decryption for each round, wherein the variable key size is one of 128, 192, and 256 bits; and

> a block round unit receiving the converted data blocks from the control unit, receiving the key from the key schedule unit encrypting or decrypting the received data blocks, and providing the encrypted or decrypted data blocks to the control unit,
>
> wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

Wasilewski relates to a method for providing conditional access information to decoders in a multiplex communications system. Daemen describes the mathematical basis and implementation aspects of the Rijndael cipher.

Wasilewski, however, does not disclose the encryption/decryption algorithm in detail. Daemen teaches the encryption/decryption algorithm independent of any device or structure for using the algorithm. For example Daemon does not disclose and teach how to process the expanding keys generated for each round of encryption/decryption in the key schedule unit. Accordingly, Wasilewski and Daemen, either individually or in combination, fail to teach "the key schedule unit provid[ing] the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit."

This limitation is added to each of independent claims 1, 10, and 22, and because Wasilewski and Daemen fail to teach all the elements of the independent claims, a *prima facie* case for obviousness has not been made. In addition, the secondary reference of Mroczkowski also fails to teach this limitation.

Claim 4 has been cancelled, and applicant believes the 103(a) rejection of claim 4 is now moot.

As set forth in MPEP 2143, to show a *prima facie* case for obviousness, all the prior art references, either individually or combined, must teach all the claim

limitations. Wasilewski or Daemen, individually or in combination, fail to teach the "the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit." Applicant submits that a *prima facie* case for obviousness has not been shown and that claims 1, 10, and 22 are patentable over the cited prior art. Additionally, claims 2-3, 5-9, 11-21, and 22-24 are patentable at least by virtue of dependence upon a patentable independent claim.

As set forth in MPEP 2131, to anticipate a claim, the reference must teach every element of the claim. None of the cited references teach the limitations of newly added independent claim 25, and applicant believes this claim is patentable over the sited art as are dependent claims 26-27 for at least the reason of depending from a patentable independent claim.

CONCLUSION

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain at issue which the Examiner feels may be best resolved through a telephone interview, the Examiner is kindly invited to contact the undersigned at (213) 623-2221.

Respectfully submitted,
Lee, Hong, Degerman, Kang & Schmadeka

Date: March 24, 2008

By: _____
Craig W. Schmoyer
Registration No. 51,007
Attorney for Applicant(s)

Customer No. 035884